COLOCVIU STRATEGIC

Nr.4/2017
(vol.146)

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

IMPLICAȚII DE SECURITATE ALE MALWARE-ULUI W32.STUXNET

Robert DRAGOŞ

Abstract: *Cyberspace generates opportunities, however it can also pose a strategic challenge for states if inadequate measures are taken to secure their national cyberinfrastructure. With Stuxnet introducing a new type of attack, the cyber-physical attack, it is necessary that states reconsider their priorities regarding national security. The article aims to present the case of W32.Stuxnet malware and the security challenges posed by such a threat. History's first field experiment in cyber-physical weapon technology resulted in destruction of 1000 centrifuges at the Fuel Enrichment Plant at Natanz, Iran. The reaction triggered by this event was an extensive Iranian campaign between late 2011 and mid-2013 of over 176 days of distributed denial of service attacks against institutions in the U.S. financial sector, additionally the campaign included compromising critical controls of a New York dam. It also has to be reminded the attack in 2012 on the computer network of Saudi Aramco, world's largest oil producer. Considering everything mentioned, questions emerge regarding whether or not such an approach is much more dangerous than a nuclear weapon.*

Keywords: *cyberspace, malware, Stuxnet, cyber-physical attack, Iran.*

Introducere

Spațiul cibernetic generează oportunități de dezvoltare, dar poate constitui, în acelaşi timp, o vulnerabilitate strategică. Atacurile cibernetice tot mai dezvoltate şi agresive determină o conştientizare la nivel internațional a importanței majore a domeniului în cauză, fiind necesară depăşirea stadiului implementării unor standarde minimale procedurale şi de securitate pentru infrastructurile cibernetice.

Apariția atacurilor cibernetice capabile să aducă distrugeri în cadrul realității obiective, aşa-numitele „cyber-physical attacks”, conduc la necesitatea reevaluării priorităților în domeniul securității naționale a statelor. Atacurile respective sunt complexe şi implică, de asemenea, resurse umane specializate în sectorul țintă.

În acest sens, trebuie menționată atenția acordată spațiului cibernetic de către organizații internaționale precum:

- Organizația Tratatului Nord-Atlantic, prin Angajamentul Aliat de Apărare Cibernetică din iulie 2016, Acordul Tehnic privind cooperarea în domeniul cibernetic între structurile specializate

***Robert DRAGOŞ** este masterand al Programului de studii „Ştiințe Penale" din cadrul Facultății de Drept, Universitatea „Titu Maiorescu" din Bucureşti şi absolvent al unui stagiu de voluntariat în cadrul Centrului de Studii Strategice de Securitate şi Apărare al Universității Nationale de Apărare „Carol I”.*

ale NATO (NATO Computer Incident Response Capability – NCIRC), respectiv UE (Computer Emergency Response Team of the European Union – CERT-EU) din februarie 2016;

- Uniunea Europeană, prin Strategia de Securitate Cibernetică a Uniunii Europene din februarie 2013 şi Directiva (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune.

Ca o completare la cele precizate, în iulie 2016, NATO a recunoscut spaţiul cibernetic drept domeniu operaţional în care Alianţa trebuie să se apere la fel de eficient precum în spaţiul aerian, terestru şi maritim[1].

La nivel naţional, trebuie precizată Hotărârea nr. 271 din 15 mai 2013 pentru aprobarea Strategiei de Securitate Cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului Naţional de Securitate Cibernetică. În cadrul Strategiei,în al treilea paragraf din Capitolul I, este definit spaţiul cibernetic ca fiind mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta[2].

Prin urmare, cercetările în acest domeniu sunt de relevanţă şi actualitate atât pentru mediul internaţional de securitate, pentru cel regional, cât şi cel naţional. Astfel, în cele ce urmează, cercetarea evidenţiază faptul că elementele infrastructurilor cibernetice nu sunt întotdeauna capabile să reziste unui atac cibernetic, fiind necesare resurse majore pentru a reveni la starea de normalitate.

1. Virusul W32.Stuxnet. Apariţie şi răspândire

W32.Stuxnet este un malware complex de dimensiuni mari, aproximativ 15000 mii de linii de cod (lines of code – LOC)[3], rezultând a fi de 20 de ori mai mare decât media, cu o multitudine de componente şi funcţii diferite[4]. Malware, termen a cărui denumire completă este „malicious software" sau „software rău intenţionat", reprezintă un program realizat cu scopul de a infecta computerul unui anumit utilizator (user) şi de a îl vătăma în diferite moduri[5]. Malware-ul în cauză a fost creat în primul rând pentru a ţinti sistemele de control industrial sau un set de sisteme similare.

Scopul acestuia a fost de a reprograma sistemele de control industrial (industrial control systems – ICS) prin modificarea codului controlerelor logice programabile (programmable logic controllers – PLCs) astfel încât acestea să funcţioneze conform indicaţiilor atacatorului, disimulând, în acelaşi timp respectivele modificări faţă de operatorul echipamentului în cauză[6].

Stuxnet a fost decoperit la 17 iunie 2010 de către Sergey Ulasen[7], programator la VirusBlokAda, o companie locală de antivirus din Minsk, Belarus, în urma sesizării realizate de un client din Iran, care raporta BSoD-uri (Blue Screen of Death) arbitrare şi reporniri ale computerelor. Iniţial, s-a suspectat a fi un conflict la nivelul programelor instalate. Ulterior, după ce s-a constatat faptul că respectiva problemă există şi la nivelul sistemelor informatice[8] pe care a fost proaspăt instalat sistemul de operare Windows şi au fost examinate cu atenţie aplicaţiile, s-a ajuns la concluzia că nucleul problemei este un malware. Odată ce a fost localizat malware-ul, a fost supus analizei, din care a reieşit faptul că acesta folosea vulnerabilităţi de tipul 0-day[9], precum şi faptul că driverele Stuxnet erau semnate cu un certificat digital[10] aparţinând Realtek Semiconductor Corp. La acel moment, Ulasen, prin intermediul VirusBlokAda, a emis un avertisment unde descria situaţia de fapt şi preciza modul de operare al malware-ului.

Conform celor expuse, W32.Stuxnet instalează două drivere:

- *„mrxcls.sys"* – acţionează ca punct principal de încărcare pentru malware (loadpoint), permiţând ca Stuxnet să fie executat ori de câte ori un sistem infectat este bootat[11]
- *„mrxnet.sys"* – folosit pentru a ascunde fişierele maliţioase pe computerul compromis[12].

După cum am precizat, ambele drivere erau semnate cu un certificat digital aparţinând Realtek Semiconductor Corp. Revocarea certificatului s-a realizat în data de 16 iulie 2010 de Verisign. Ulterior ESET descoperă la 17 iulie 2010 o versiune diferită a driver-ului „mrxcls.sys", de această dată semnat cu un certificat digital aparţinând JMicron Technology Corp. Revocarea certificatului în cauză s-a realizat în 5 zile, de către Verisign, la 22 iulie 2010[13].

Măsura revocării certificatelor menţionate a avut ca rezultat numai eliminarea posibilităţii de a mai semna alte drivere cu certificate digitale aparţinând Realtek şi JMicron, precum şi sublinierea faptului că niciuna din companiile în cauză nu susţin o asemenea conduită. Prin urmare, măsura respectivă nu afectează în niciun mod funcţionarea malware-ului.[14]

Stuxnet prezintă numeroase caracteristici, precum:

- se reproduce prin intermediul drive-urilor detaşabile, exploatând o vulnerabilitate care permite executarea automată;

- se răspândeşte într-o reţea LAN (Local Area Network) prin intermediul unei vulnerabilităţi din cadrul Windows Print Spooler, un fişier executabil care gestionează procesul de printare[15];
- se răspândeşte prin SMB (Server Message Block), un protocol pentru partajarea resurselor, precum fişiere, imprimante, cu mai mult de un dispozitiv într-o reţea[16], prin exploatarea unei vulnerabilităţi din cadrul Windows Server Service;
- se actualizează printr-un mecanism peer-to-peer în cadrul unui LAN;
- exploatează patru vulnerabilităţi de tipul 0-day;
- poate fi controlat printr-un server de comandă şi control;
- conţine un Windows rootkit, astfel ascunzând fişierele copiate pe drive-urile detaşabile, ceea ce împiedică utilizatorul să sesizeze faptul ca drive-ul detaşabil a fost infectat înainte ca acesta să îl transfere mai departe unui alt utilizator;
- ascunde codul modificat pe PLC-uri.

În ceea ce priveşte infecţia propriu-zisă, unul dintre primii paşi pe care W32.Stuxnet îi realizează este să determine dacă pe sistemul informatic rulează o versiune Windows pe 32 de biţi sau pe 64 de biţi.

În cazul în care pe computer rulează o versiune Windows pe 64 de biţi, nu există niciun pericol. De asemenea, Stuxnet operează numai pe anumite sisteme de operare, în speţă: Win2K, WinXP, Windows 2003, Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2. Ulterior, malware-ul verifică: dacă este deja infectat computerul; dacă are privilegii de administrator, Stuxnet vrând să aibă permisiunea de a realiza orice acţiune; ce fel de antivirus este instalat pe computerul respectiv şi care este cel mai potrivit proces pentru injectare, precum: lsass.exe, winlogon.exe, svchost.exe, proce-sele sofware-urilor de securitate instalate[17].

Numărul mare de infectări în Iran (figura nr.1), indică faptul că, cel mai probabil, acesta era ţinta principală.

Primele cinci atacuri ale Stuxnet s-au realizat asupra unor companii de origine iraniană aflate în legătură cu programul nuclear iranian, de aici rezultând implicaţii de securitate. Toate companiile în cauză activează în domeniul sistemelor de automatizare industrială, cu excepţia Kalaye Electric Company.

Companiile afectate, care se pot identifica şi prin intermediul figurii nr. 2, sunt după cum urmează: Foolad Technic Engineering Company – Domeniul A; Behpajooh Co. Elec & Comp. Engineering – Domeniul B; Neda Industrial Group – Domeniul C; Control-Gostar Jahed Company – Domeniul D; Kalaye Electric Company – Domeniul E[18].

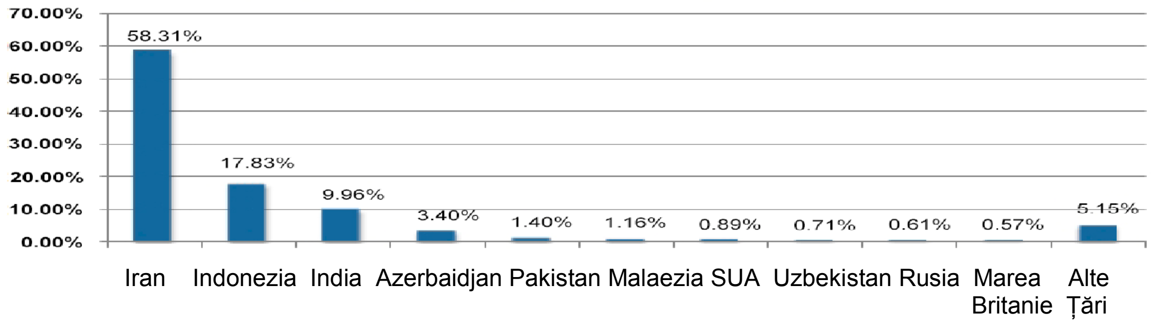


Figura nr. 1: Distribuţia geografică a numărului de infecţii. *Sursa: Symantec.com*

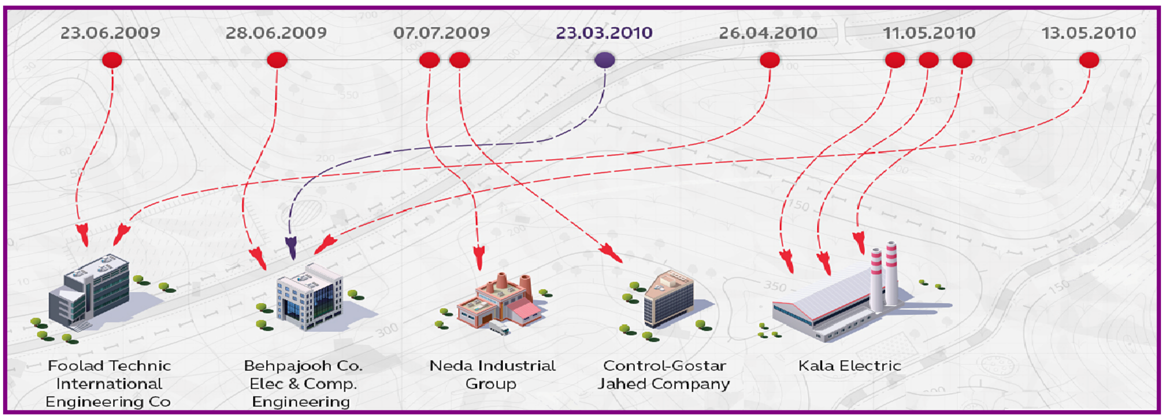


Figura nr. 2: Cronologia atacurilor asupra celor cinci companii iraniene. *Sursa: Kaspersky.com*

▪ Foolad Technic Engineering Company – Domeniul A – a fost prima companie atacată, la 23 iunie 2009. Atacul în cauză a fost cel mai rapid dintre cele 10 atacuri executate asupra celor 5 companii (tabel nr. 1), infectarea producându-se în 12 ore. Ulterior, compania a fost din nou atacată, la 26 aprilie 2010, intrând sub incidenţa celui de-al treilea val de infecţii.

▪ Behpajooh Co. Elec & Comp. Engineering – Domeniul B – a fost atacată de trei ori, o dată în 2009 şi de două ori în 2010. Primul atac s-a executat la 28 iunie 2009, infectarea realizându-se în 6 zile şi 6 ore. Varianta Stuxnet al celui de-al doilea atac din data de 23 martie 2010, clasificat ca fiind cel mai eficient dintre cele 10 atacuri, a fost responsabilă pentru un procentaj de 69% de infectări din totalul celor 12000 care au avut loc asupra entităţilor în cauză[19]. Infectarea Domeniului B în cadrul celui de-al doilea atac s-a realizat în 22 de zile. Trebuie precizat faptul că cel de-al doilea atac asupra Domeniului B a avut repercusiuni majore privind răspândirea Stuxnet, atât la nivelul Iranului, cât şi la nivel global. Al treilea atac şi cel mai lent a avut loc la 13 mai 2010, infectarea producându-se în 28 de zile şi 18 ore.

▪ Kalaye Electric Company[20] – Domeniul E – a fost o companie privată, ulterior achiziţionată de Organizaţia pentru Energie Atomică din Iran, care a constituit principala zonă de cercetare şi dezvoltare a centrifugelor, până la transferarea operaţiunilor la Natanz în 2002. „Kalaye Electric" are înţelesul de „bunuri electrice". Considerăm că menţinerea denumirii după achiziţionare ar fi putut avea drept scop disimularea activităţii respectivei entităţi. KEC a fost singura entitate atacată de trei ori, la aceeaşi dată, toate atacurile producându-se în luna mai, ultimul atac având loc la un interval de 17 secunde faţă de cel anterior. Astfel, primul atac a avut loc în data de 11 mai 2010, infectarea producându-se în 26 de zile şi 19 ore. Al doilea atac a avut loc la aceeaşi dată, în speţă 11 mai 2010, infectarea realizându-se în 27 de zile. Al treilea atac şi ultimul, de la aceeaşi data 11 mai 2010, după cum am precizat anterior, s-a realizat la 17 secunde faţă de cel anterior.

Eric Chien şi Liam O'Murchu, specialişti din cadrul Symantec Security Response, consideră că atacurile realizate asupra celor cinci companii menţionate anterior nu au reprezentat un efect advers al Stuxnet în ceea ce priveşte răspândirea malware-ului. Din contră, aceştia expun faptul că atacatorii aveau informaţii din care rezulta faptul că tehnicienii care activau la companiile în cauză, lucrau şi la uzina de îmbogăţire a uraniului de la Natanz (figura nr. 3): „[Atacatorii] ştiau că tehnicienii de la aceste companii vor vizita Natanz. Prin urmare, aceştia vor infecta aceste companii şi ulterior tehnicienii îşi vor lua computerul sau laptopul ori USB-ul"[21] „şi vor merge la Natanz unde vor introduce USB-ul, care are un cod pe care trebuie să îl încarce în Natanz, iar acum Stuxnet are posibilitatea să pătrundă în cadrul Natanz şi să îşi desfăşoare atacul"[22].„Aceste cinci companii au fost ţintite cu scopul de a introduce şi răspândi Stuxnet în Natanz"[23]. Astfel, rezultă că s-a urmărit infectarea echipamentelor tehnicienilor respectivi, precum laptopurile, USB-urile acestora, finalitatea fiind atacarea uzinei de îmbogăţire a uraniului de la Natanz. Despre uzina în cauză s-a afirmat că este izolată de Internet.[24]Este important în a se preciza faptul că nu trebuie să existe în niciun moment iluzia că dacă un sistem informatic nu este conectat la Internet, acesta nu poate fi atacat.

Valul de Atac	Domeniul Atacat	Momentul Producerii Infecţiei	Timpul de Infectare
Valul de Atac 1	Domeniul A	23 iunie 2009 4:40:16	0 zile 12 ore
	Domeniul B	28 iunie 2009 23:18:14	6 zile 6 ore
	Domeniul C	7 iulie 2009 5:09:28	14 zile 12 ore
	Domeniul D	7 iulie 2009 9:27:09	14 zile 16 ore
Valul de Atac 2	Domeniul B	23 martie 2010 6:06:07	22 zile 0 ore
Valul de Atac 3	Domeniul A	26 aprilie 2010 9:37:36	11 zile 22 ore
	Domeniul E	11 mai 2010 6:36:32	26 zile 19 ore
	Domeniul E	11 mai 2010 11:45:53	27 zile 0 ore
	Domeniul E	11 mai 2010 11:46:10	27 zile 0 ore
	Domeniul B	13 mai 2010 5:02:23	28 zile 18 ore

Tabel nr. 1: Valurile atacurilor desfăşurate asupra ţintelor iniţiale



Figura nr. 3: Localizarea geografică a uzinei de îmbogățire a uraniului de la Natanz; *Sursă: Google.com/maps*

2. W32.Stuxnet. Un atac fizico-cibernetic

Malware-ul care face obiectul prezentei cercetări, introduce un nou tip de atacuri cibernetice,în speță atacurile fizico-cibernetice. Un asemenea atac depăşeşte limitele puterii cibernetice care nu poate cauza în mod direct o vătămare corporală sau o distrugere a bunurilor, ori să ocupe un anumit spațiu. În acest sens, credem că este important să evidențiem câteva aspecte cu privire la puterea cibernetică şi nivelurile de desfăşurare pe care le implică un atac fizico-cibernetic. Puterea cibernetică poate fi definită ca fiind abilitatea de a face uz de spațiul cibernetic pentru a crea avantaje şi a influența situații în cadrul tuturor mediilor operaționale şi în cadrul celorlalte instrumente ale puterii.[25]

Aria de aplicare a puterii cibernetice este diversificată. Astfel, puterea cibernetica poate fi privită ca: **1.** un instrument puternic de colectare a informației; **2.** un factor perturbator în ceea ce priveşte rețeaua inamicului; **3.** un factor demoralizator asupra inamicului, mai ales având în vedere celeritatea publicității contemporane[26].

Prin trimitere la cele expuse anterior, un atac fizico-cibernetic implică o desfăşurare pe trei niveluri (fig. nr. 4): 1. nivelul IT, folosit pentru a propaga malware-ul; 2. nivelul sistemului de control industrial, utilizat pentru manipularea (cu precizarea că nu se face referire la perturbare) controlului asupra procesului; 3. nivelul fizic, zona unde are loc distrugerea.

Atacul de la uzina de îmbogățire a uraniului de la Natanz a avut drept rezultat distrugerea a 1000 de centrifuge[27] prin schimbarea vitezei de rotație a rotorului centrifugei, inițial prin creşterea vitezei de la 63000 de mii de rotații pe minut (rpm) la 84600 de mii rpm, ulterior scăderea acesteia la 120 rpm[28]. Datele transmise către operatori erau cele înregistrate în regim normal de funcționare al centrifugelor. Astfel, operatorii respectivi se aflau în necunoştință de cauză cu privire la situația curentă.

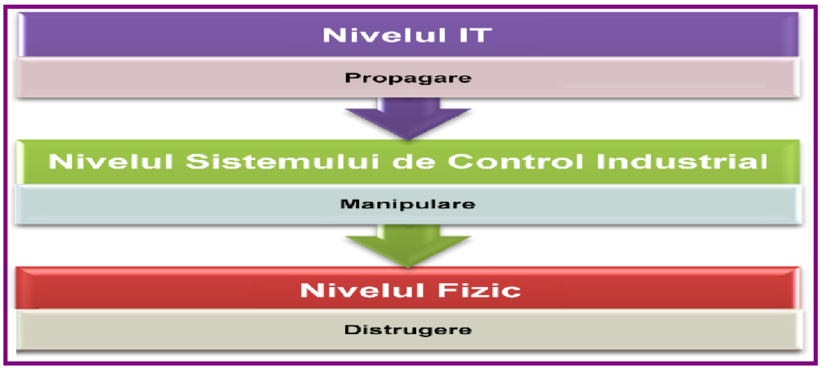


Figura nr. 4: Nivelurile unui atac fizico-cibernetic; *Sursa: Langner.com*

3. Operațiunea „Jocurile Olimpice” şi poziția Iranului

Conform Stratfor, există posibilitatea ca Stuxnet să fi fost rezultatul unei cooperări operaționale extinse dintre Statele Unite ale Americii şi Israel[29]. Literatura de specialitate precizează faptul că numele de cod al operațiunii speciale privind Stuxnet ar fi purtat denumirea de „Jocurile Olimpice”, element din cadrul unui program de război cibernetic de lungă durată început în timpul administrației George W. Bush[30]. Încă din 2002, George W. Bush afirma faptul că unul din scopurile SUA este de a împiedica regimurile care sponsorizează teroarea să formuleze amenințări cu arme de distrugere în masă la adresa Americii sau a prietenilor şi aliaților acesteia. În continuare, acesta preciza faptul că Iranul urmăreşte agresiv dobândirea acestor tipuri de arme şi faptul ca exportă teroare.[31]

Considerăm că, în funcție de scopul urmărit de atacator, precum testarea de noi tehnologii, încetinirea dezvoltării programului nuclear iranian, distrugerea integrală a tuturor centrifugelor, acțiunile întreprinse se vor putea aprecia ca având succes sau ca fiind un eşec.

Iranul nu a admis faptul că a fost afectat de Stuxnet şi nu a adoptat, public, nicio poziție în acest sens.

Gary D. Brown identifică o serie de posibili factori care ar fi putut influența această lipsă de reacție la nivel public cu privire la atacurile realizate, precum: sancțiunile impuse la nivel internațional privind programul său nuclear; factorul demoralizator pe care îl poate avea asupra națiunii, având în vedere multitudinea de măsuri de securitate şi de disimulare a activității întreprinse; dificultatea în identificarea făptuitorului şi implicit reticența în a nominaliza entitatea suspectă de atac, existând riscul creşterii agresivității atacatorului; colectarea de informații cu privire la atacator şi modurile acestuia de operare[32].

Deşi public, Iranul nu a adoptat nicio poziție privind Stuxnet, la sfârşitul anului 2011 a lansat o serie de atacuri informatice direcționate împotriva Statelor Unite ale Americii, atacuri care au continuat până la mijlocul anului 2013. Ținta atacurilor a fost mai exact sistemul bancar şi Saudi Aramco, cel mai mare producător de petrol din lume[33].

Conform informațiilor Biroului Federal de Investigații (Federal Bureau of Investigation – FBI) şapte funcționari aparținând a două companii iraniene, în speță ITSecTeam şi Mersad Company, sponsorizate şi direcționate de guvernul iranian, au executat atacuri la diferite intervale de timp. Astfel, între anul 2011 şi anul 2013, 46 de instituții aparținând sectorului financiar al SUA s-au aflat sub incidența acestor atacuri. De asemenea acțiunile au inclus şi compromiterea sistemelor de Monitorizare, Control şi Achiziție de Date (Supervisory Control and Data Acquisition – SCADA) ale barajului Bowman din New York[34]. În total, au rezultat peste 176 de zile de atacuri de tip blocarea distribuită a serviciului (Distributed Denial of Service – DDoS)[35].

În august 2012, rețeaua companiei Saudi Aramco a fost atacată de un malware intitulat Shamoon, cauzând infectarea a 30.000 de sisteme informatice care operau prin Windows. Vătămarea adusă companiei a fost considerabilă, necesitând aproximativ două săptămâni pentru a restabili funcționarea acesteia în regim normal. Malware-ul Shamoon urmăreşte ştergerea integrală a datelor de pe computerul infectat[36], astfel afectând la acel moment sectorul de afaceri al Saudi Aramco. Shamoon a acționat şi asupra altor companii, exemplu în acest sens fiind RasGas[37].

Reacția complexă şi agresivă în fapt, chiar dacă neasumată public, a Iranului demonstrează faptul că, în primul rând, acesta alocă tot mai multe resurse în sectorul spațiului cibernetic şi faptul că şi-a exprimat public intenția de a intra în rândul statelor foarte dezvoltate în domeniu, precum: SUA, India, Marea Britanie, Israel, Rusia, Germania, Franța, China, Coreea de Sud[38].

Procurorul SUA al Districtului de Sud din New York, Preet Bharara, a făcut o precizare importantă în urma atacurilor comise asupra sistemului bancar american şi asupra barajului Bowman: „Trăim, în acest moment, într-o lume unde atacuri devastatoare pot fi lansate din orice parte a lumii, numai cu un click al mouse-ului, asupra sistemului nostru financiar, infrastructurii noastre şi asupra modului nostru de viață”[39].

Concluzii

Atacurile fizico-cibernetice au devenit o realitate prin intermediul malware-ului complex W32.Stuxnet. În acest sens, este important în a se observa câteva aspecte.

În primul rând, creatorii malware-ului au avut informații precise privind entitatea care a făcut obiectul atacului, prin urmare sprijin din partea resurselor umane specializate în sectorul țintă. În continuare, s-a depăşit impedimentul reprezentat de sistemele informatice izolate, fără acces la internet.

De asemenea, s-au exploatat patru vulnerabilități de tipul 0-day şi s-a făcut uz de două certificate digitale furate. Este necesar să se precizeze faptul că Stuxnet a fost proiectat astfel încât să acționeze numai asupra unei anumite configurații software şi hardware.

Luând în considerare resursele colosale necesare pentru realizarea Stuxnet, precum şi creativitatea de care s-a dat dovadă în proiectarea acestuia, am putea ajunge la concluzia că numai câteva state din lume ar avea capacitatea de a realiza un asemenea malware.

Având în vedere cele expuse, se pune întrebarea dacă nu cumva o asemenea abordare este mult mai periculoasa decât armamentul nuclear.

NOTE:

[1]***, „Cyber defence", North Atlantic Treaty Organization, 2017, URL:http://www.nato.int/cps/en /natohq/ topi cs_78170.htm, accesat la data de 22 iunie 2017.

[2]***, „Strategia de Securitate Cibernetică a României", Guvernul României, 2013, URL: http://legislatie.just.ro/ Public/DetaliiDocument/148324, accesat la data de 23 mai 2017.

[3] Ralph Langner, „CrackingStuxnet, a 21st-century cyberweapon", March 2011, URL: https://www.ted.com /talks/ralph_langner_cracking_stuxnet_a_21st_century_cy berweapon/transcript, accesat la 17 mai 2017.

[4] Nicolas Falliere, Liam O'Murchu, Eric Chien, „W32. Stuxnet Dossier, Version 1.4", Symantec Corporation, 2011, p. 1, URL: https://www.symantec. com/content /en/us/enterprise/media/security_response/whitepapers/w 32_stuxnet_dossier.pdf, accesat la 17 mai 2017.

[5] Kaspersky Lab US, „Whatis Malware and How to Protect Against It?", URL: https://usa.kaspersky.com /resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it, accesat la 17 mai 2017.

[6] Nicolas Falliere, Liam O'Murchu, Eric Chien, 2011, *op. cit.*, p. 1.

[7] Eugene Kaspersky, „Interviewwith Sergey Ulasen, The Man Who Found The StuxnetWorm", November 2, 2011, URL: https://eugene.kaspersky.com/2011/11/02/ the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight, accesat la 18 iunie 2017.

[8] Noul Cod Penal, art. 181 Sistem informatic şi date informatice.

(1) Prin sistem informatic se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.

Într-o accepțiune mai simplă, sistemul informatic este compus din entități materiale, precum elemente hardware şi elemente software.

Vasile Dobrinoiu, Ilie Pascu, Mihai Adrian Hotca, „Noul Cod Penal comentat, Partea specială", Ed. a III-a revăzută şi adăugită, Ed. Universul Juridic, Bucureşti, 2016, pp. 868.

[9] Roger Park, „Guideto Zero-Day Exploits", Symantec Connect Community, 9 noiembrie 2015, URL: https:// www.symantec.com/connect/blogs/guide-zero-day-expl oits, accesat la 22 mai 2017.

Vulnerabilitatea de tip 0-day este o vulnerabilitate de aplicație necunoscută developer-ului, expresia punând în evidență faptul că developer-ul are „zero zile" la dispoziție pentru a rezolva problema dezvăluită şi posibil deja exploatată. Astfel, persoane rău intenționate care află despre existența unor asemenea vulnerabilități le vor exploata până în momentul în care developer-ul va găsi o cale să le înlăture.

[10]*Semnătura digitală este un termen utilizat cu privire la marcarea sau semnarea unui document electronic. Scopul semnăturii digitale este de a asigura veridicitatea identității semnatarului, integrității datelor acestuia, precum şi de a face imposibilă repudierea semnăturii unui document.*

Pentru a putea crea o semnătură digitală este nevoie de un certificat digital emis de o Autoritate de Certificare (Certificate Authority – CA), o entitate administrativă centrală de încredere care poate emite certificate digitale utilizatorilor şi serverelor, exemplu în acest sens este Verisign, Entrust, precum şi alte autorități. Astfel, certificatul serveşte la probarea identității entității semnatare.

Entrust, „Digital Signatures", URL: https://www.entrust. com/digital-signatures, accesat la 19 iunie 2017.

Microsoft, „What is a digital signature?", URL: https://technet.microsoft.com/en-us/library/cc545901 (v =office.12).aspx, accesat la 19 iunie 2017.

IBM Knowledge Center, „CA (autoritate de certificare)", URL: https://www.ibm.com/support/knowledgecenter/ro /ssw_i5_54/rzahu/rzahurzahu02mcertificateauthority.htm, accesat la 19 iunie 2017.

Microsoft, „Digital Signatures and Certificates", URL: https://support.office.com/en-us/article/Digital-signature s-and-certificates-8186cd15-e7ac-4a16-8597-22bd163 e8e96, accesat la 19 iunie 2017.

[11] Nicolas Falliere, Liam O'Murchu, Eric Chien, 2011, *op. cit.*, p. 20.

[12] Nicolas Falliere, Liam O'Murchu, Eric Chien, 2011, *op. cit.*, p. 18.

Alexander Gostev, Igor Soumenkov, „Stuxnet/Duqu: The Evolution of Drivers", 28 decembrie 2011, URL: https://securelist.com/analysis/publications/36462/stuxnetd uqu-the-evolution-of-drivers, accesat la 21 mai 2017.

VirusBlokAda, „Rootkit.TmpHider", URL: http://anti-vir us.by/en/tempo.shtml, accesat la 19 iunie 2017.

Aleksandr Matrosov, Eugene Rodionov, David Harley, Juraj Malcho, „Stuxnet Under the Microscope, Revision 1.1", ESET, pp. 52-56, URL:https://www.esetnod32.ru/ company/viruslab/analytics/doc/Stuxnet_Under_the_Micro scope.pdf, accesat la 27 iunie 2017.

[13] Nicolas Falliere, Liam O'Murchu, Eric Chien, 2011, *op. cit.*, pp. 4.

[14]Costin Raiu, „Stuxnet signed certificates frequently asked questions", Securelist, July 21, 2010, URL: https://securelist.com/stuxnet-signed-certificates-freque ntly-asked-questions/29725, accesat la 19 iunie 2017.

Chester Wisniewski, „Certified uncertainty, Naked Security, 20 July 2010, URL: https://nakedsecurity.sop hos.com/2010/07/20/certified-uncertainty, accesat la 19 iunie 2017.

[15]***, „Print Spooler", Microsoft URL: https://msdn.micr osoft.com/en-us/library/windows/desktop/dd162871(v= vs.85).aspx, accesat la 18 mai 2017.

[16]***, „Configurarea SMB", Canon URL: http://ug.oipsrv. net/USRMA-2429-zz-CS-roRO/contents/CS3025_setu p_0036.html, accesat la 20 mai 2017.

[17] Nicolas Falliere, LiamO'Murchu, Eric Chien, „W32.Stuxnet Dossier, Version 1.4", Symantec Corporation, 2011, pp. 14-16, URL: https://www.syman tec.com/content/en/us/enterprise/media/security_response /whitepapers/w32_stuxnet_dossier.pdf, accesat la 17 mai 2017.

[18]***, „Stuxnet: Zero Victims", Kaspersky Lab's Global Research & Analysis Team, 11 noiembrie 2014, URL: https://securelist.com/stuxnet-zero-victims/67483, accesat la 19 iunie 2017.

[19] Nicolas Falliere, Liam O'Murchu, Eric Chien, 2011, *op. cit.,* pp. 11, URL: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, accesat la 17 mai 2017.

[20]***, „Kalaye Electric Company", Wisconsin Project on Nuclear Arms Control, URL: http://www.iranwatch.org/iranian-entities/kalaye-electric-company, accesat la 21 mai 2017.

***, „ImageryBrief: Kalaye Electric", Institute for Scienceand International Security, 31 martie 2005, URL: http://isis-online.org/isis-reports/detail/isis-imagery -brief-kalaye-electric/8, accesat la 18 iunie 2017.

***, „Kalaye Electric Company", Institute for Scienceand International Security, URL: http://www.isisnucleariran.org/sites/detail/kalaye, accesat la 18 iunie 2017.

[21]Liam O'Murchu, *„Zero Days", Documentary*, 2016.

[22]Eric Chien, *„Zero Days", Documentary*, 2016.

[23] Liam O'Murchu, *„Zero Days", Documentary*, 2016.

[24]Brian Donohue, „Army Looking for Ways to Infiltrate Air-Gapped Systems", Threatpost, URL: https://threat post.com/army-looking-ways-infiltrate-air-gapped-systems-011713/77421, accesat la 22 iunie 2017.

[25] Daniel T. Kuehl, „From Cyber space to Cyber power: Defining the Problem", Center for Technology and National Security Policy, US Department of Defense, URL: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf, pp. 12, accesat la 26 mai 2017.

Arthur Lazăr-Mureşan, „Revoluția tehnologică, mega trendul începutului de secol XXI", Revista Intelligence, Serviciul Român de Informații, 30 iunie 2016, URL: http://intelligence.sri.ro/revolutia-tehnologica-mega-trendul-inceputului-de-secol-xxi, accesat la 26 mai 2017.

[26]Lukas Milevski, „Stuxnet and Strategy: A Special Operation în Cyberspace?", Joint Force Quarterly, Issue 63, 4th Quarter, National Defense University Press, St. Louis, Missouri, 2011, pp. 65, URL: http://www.dtic.mil/doctrine/jfq/jfq-63.pdf, accesat la 9 aprilie 2017.

[27]*Uraniul, în starea sa naturală, este constituit în proporție de 99.3% din uraniu-238, 0.7% fiind uraniu-235. În funcție de scopul urmărit, concentrația sau îmbogățirea izotopului 235 trebuie să fie adusă la un procent de 3-5% pentru un reactor nuclear şi la un procent 80-95% pentru o armă nucleară. În acest sens, cu ajutorul centrifugei, tub cilindric care este rotit în jurul axei sale la viteze foarte mari, se colectează uraniu-235.*

***, „Uranium Enrichment", U.S. Nuclear Regulatory Commission, URL: https://www.nrc.gov/materials/fuel-cycle-fac/ur-enrichment.html, accesat la 21 iunie 2017.

Ivan Oelrich, Ivanka Barzashka, „Centrifuge Basics", Federation of American Scientists, URL:https://fas.org/programs/ssp/nukes/fuelcycle/centrifuges/centrifuge.html, accesat la 21 iunie 2017.

Houston G. Wood, Alexander Glaser, R. Scott Kemp, „The gas centrifuge and nuclear weapons proliferation", Princeton University, 2008, URL: https://www.princeton.edu/~rskemp/Kemp%20-%20Gas%20Centrifuge%20and%20Nonproliferation%20-%20SPLG.pdf, accesat la 21 iunie 2017.

Dan Plăvițu, „Războiul Cibernetic - de la posibilitate la realitate", Infosfera, Anul III nr. 2/2011, Direcția Generală de Informații a Apărării, pp. 12, URL: http://www.mapn.ro/publicatii/2_2011.pdf, accesat la 20 mai 2017.

[28] Ralph Langner, „To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve", The Langner Group, November 2013, pp. 12, URL: https://www.langner.com/wp-content/uploads/2017/03/ to-kill-a-centrifuge.pdf, accesat la 23 aprilie 2017.

[29]Stratfor, „The U.S.-Israeli Stuxnet Alliance",January 17, 2011, URL: https://www.stratfor.com/analysis/us-isr aeli-stuxnet-alliance, accesat la 26 mai 2017.

[30] Robert J. Reardon, „Containing Iran: Strategies for Addressingthe Iranian Nuclear Challenge", RAND Corporation, 2012, pp. 131, URL: http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1180.pdf, accesat 28 mai 2017.

Ralph Langner, 2013, *op. cit.,* pp. 16, URL: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf, accesat la 23 aprilie 2017.

[31]The White House, „President Delivers State of the Union Address", January 29, 2002, URL: https://georgewbush-whitehouse.archives.gov/news/releases/2002/01/20020129-11.html, accesat la 16 iunie 2017.

[32] Gary D. Brown, „Why Iran Didn't Admit Stuxnet Was an Attack", Joint Force QuarterlyIssue 63, 4th Quarter, National Defense University Press, St. Louis, 2011, pp. 71-73, URL: http://www.dtic.mil/doctrine/jfq/jfq-63.pdf, accesat la 9 aprilie 2017.

[33] Martin C. Libicki, „Iran: A Rising Cyber Power?", RAND Corporation, December 16, 2015, URL: http://www.rand.org/blog/2015/12/iran-a-rising-cyber-power.html, accesat la 18 iunie 2017.

[34]***, „Iranians Charged with Hacking U.S. Financial Sector", Federal Bureau of Investigation, March 24, 2016, URL: https://www.fbi.gov/news/stories/iranians-charged -with-hacking-us-financial-sector, accesat la 18 iunie 2017.

[35]***, „Seven Iranians Working for Islamic Revolutionary Guard Corps – Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector", US Department of Justice, March 24, 2016, URL: https://www.justice.gov/ opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged, accesat la 18 iunie 2017.

[36] Costin Raiu, Mohamad Amin Hasbini, Sergey Belov, Sergey Mineev, „From Shamoon to Stone Drill", Secure list, March 6, 2017, URL: https://securelist.com/from-shamoon-to-stonedrill/77725, accesat la 18 iunie 2017.

[37] Christopher Bronk, Eneken Tikk - Ringas, „The Cyber Attack on Saudi Aramco", International Institute for Strategic Studies, 1 April 2013, URL: http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival --global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272, accesat la 18 iunie 2017.

[38]***, „The Stuxnet Computer Wormandthe Iranian Nuclear Program", Stratfor, 24 septembrie 2010, URL: https://www.stratfor.com/analysis/stuxnet-computer-worm-and-iranian-nuclear-program, accesat la 21 iunie 2017.

[39]***, „Seven Iranians Working for Islamic Revolutionary Guard Corps – Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector", US Department of Justice, 24 martie 2016, URL: https://www.justice.gov/ opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged, accesat la 18 iunie 2017.

CONCLUZII:

Atacurile fizico-cibernetice au devenit o realitate prin intermediul malware-ului complex W32.Stuxnet. În acest sens, este important a se observa câteva aspecte. În primul rând, creatorii malware-ului au avut informații precise privind entitatea care a făcut obiectul atacului, prin urmare sprijin din partea resurselor umane specializate în sectorul țintă. În continuare, s-a depăşit impedimentul reprezentat de sistemele informatice izolate, fără acces la internet. De asemenea, s-au exploatat patru vulnerabilități de tipul 0-day şi s-a făcut uz de două certificate digitale furate. Este necesar să se precizeze faptul că Stuxnet a fost proiectat astfel încât să acționeze numai asupra unei anumite configurații software şi hardware.

Luând în considerare resursele colosale necesare pentru realizarea Stuxnet, precum şi creativitatea de care s-a dat dovadă în proiectarea acestuia, putem afirma că numai câteva state din lume ar avea capacitatea de a realiza un asemenea malware.

Având în vedere cele expuse, conchidem că atacurile fizico-cibernetice reprezintă o amenințare cu implicații puternice pentru securitatea internațională.

COLOCVIU STRATEGIC *este o publicație a Centrului de Studii Strategice de Apărare şi Securitate ce prezintă principalele rezultate ale unor studii de cercetare, sintezele unor evenimente ştiințifice, opiniile şi punctele de vedere ale masteranzilor şi doctoranzilor, implicați în cercetarea ştiințifică din domeniul apărării şi securității.*

COLOCVIU STRATEGIC
Supliment al revistei Impact Strategic
Redactor: ACS Cătălina Todor
ISSN Online 1842-8096; ISSN-L 1841-7396
1383/2017

Centrul de Studii Strategice de Apărare şi Securitate
Şos. Panduri, nr. 68-72, Sector 5, Bucureşti
Telefon: 021.319.56.04, Fax 021.319.55.93
e-mail: cssas@unap.ro
http//:cssas.unap.ro